IN THE CLAIMS:

Please amend claims 1-12, 14-24, and 26-31 as follows. Please cancel claim 25 without prejudice or disclaimer. Please add new claims 32-52 as follows.

1. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message ~~for the called party~~.

2. (Currently Amended) ~~A~~ The method as claimed in claim 1, wherein the determining in the first network comprises determining the address contained in a message for said called party.

3. (Currently Amended) ~~A~~ The method as claimed in claim 2, wherein the determining in the first network comprises determining the address contained in the message comprises a packet form.

4. (Currently Amended) ~~A~~ The method as claimed in claim 1, wherein the determining if the called party is in a trusted network comprises checking if the address is contained in a database of trusted networks.

5. (Currently Amended) ~~A~~ The method as claimed in claim 4, wherein the determining if the called party is in the trusted network comprises checking if the address is contained in said database in said first network.

6. (Currently Amended) ~~A~~ The method as claimed in claim 4, wherein the determining if the called party is in the trusted network comprises checking if the address is contained in the database provided in a call session control function or a security gateway.

7. (Currently Amended) ~~A~~ The method as claimed in claim 4, wherein the determining if the called party is in the trusted network comprises checking if the address is contained in said database comprises domain names associated with the trusted networks and ~~IP~~ internet protocol addresses of the trusted networks.

8. (Currently Amended) ~~A~~ The method as claimed in claim 1, wherein said determining, in the first network, the address comprises determining if the address contains a domain name.

9. (Currently Amended) ~~A~~ The method as claimed in claim 8, wherein if a determination is made that the address does not contain the domain name, the determining, in the first network, the address comprises sending a request for the domain name.

10. (Currently Amended) ~~A~~ The method as claimed in claim 9, wherein the determining, in the first network, the address comprises sending said request to a domain name server.

11. (Currently Amended) ~~A~~ The method as claimed in claim 8, wherein if a determination is made that the address does not contain the domain name, the determining, in the first network, the address comprises assuming that the called party is in an untrusted network.

12. (Currently Amended) ~~A~~ The method as claimed in claim 1, wherein if the called party is not in the trusted network, the controlling comprises discarding at least one message for the called party.

13. (Cancelled)

14. (Currently Amended) ~~A~~ The method as claimed in claim ~~13~~1, wherein the controlling comprises modifying said at least one message for the called party by removing identity information relating to said calling party.

15. (Currently Amended) ~~A~~ The method as claimed in claim 14, wherein the controlling comprises removing said identity information comprising a p-asserted-identity header.

16. (Currently Amended) ~~A~~ The method as claimed in claim 1, further comprising:

operating said first network and a second network in accordance with session initiation protocol.

17. (Currently Amended) ~~A~~ The method as claimed in claim 1, wherein the determining if the called party is in the trusted network comprises determining if a connection from a calling network to a called network is secured.

18. (Currently Amended) ~~A~~ The method as claimed in claim 17, wherein the determining if the called party is in the trusted network is performed in a gateway of the calling network.

19. (Currently Amended) ~~A~~ The method as claimed in claim 18, wherein the determining if the called party is in the trusted network comprises determining if the connection between the gateway of the calling network and a gateway of the called network comprises a secure connection.

20. (Currently Amended) A ~~communications~~ system, comprising:

a first ~~determining unit~~ determiner configured to determine an address associated with a called party located in a second network;

a second ~~determining unit~~ determiner configured to determine based on said address if said called party is in a trusted network; and

a ~~controlling unit~~ controller configured to control communication between the called party and a calling party, located in a first network, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

21. (Currently Amended) ~~A network element~~ An apparatus, comprising:

a first ~~determining unit~~ determiner configured to determine an address associated with a called party located in ~~a second~~ another network;

a second ~~determining unit~~ determiner configured to determine, based on said address, if said called party is in a trusted network; and

a ~~controlling unit~~ controller configured to control communication between the called party and a calling party, located in ~~the network element~~ a network where the apparatus is located, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

22. (Currently Amended) A method, comprising:

determining, in a first network, if there is a secure connection with a second network; and

modifying a message from a calling party of the first network to a called party of the second network if a determination is made that there is no secure connection with said second network.

23. (Currently Amended) ~~A~~ The method as claimed in claim 22, wherein said determining is performed in a gateway.

24. (Currently Amended) ~~A~~ The method as claimed in claim 23, wherein the determining is performed in said gateway comprising a security gateway.

25. (Cancelled)

26. (Currently Amended) ~~A network element~~ An apparatus, comprising:

first determining means for determining an address associated with a called party located in ~~a second~~ another network;

second determining means for determining, based on said address, if said called party is in a trusted network; and

control means for controlling communication between the called party and a calling party based on if said called party, located in ~~the network element~~ a network where the apparatus is located, is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

27. (Currently Amended) ~~A network element~~ An apparatus, comprising:

a ~~determining unit~~ determiner configured to determine if there is a secure connection with ~~a second~~ another network; and

a ~~modifying unit~~ modifier configured to modify a message from a calling party of a network where the apparatus is located to a called party of the other network if a

determination is made that there is no secure connection with said ~~second~~ another network.

28. (Currently Amended) ~~A network element~~ An apparatus, comprising:

determining means for determining if there is a secure connection with ~~a second~~ another network; and

modifying means for modifying a message from a calling party of ~~a first network~~ a network where the apparatus is located to a called party of ~~a second~~ the another network if a determination is made that there is no secure connection with said ~~second~~ another network.

29. (Currently Amended) A method, comprising:

determining, in a gateway in a first network, if there is a secure connection with a second network; and

discarding a message from a calling party in a first network to a called party in a second network, if a determination is made that there is no secure connection with said second network.

30. (Currently Amended) ~~A network element~~ An apparatus, comprising:

a ~~determining unit~~ determiner configured to determine, in a gateway ~~in a first network~~, if there is a secure connection with ~~a second~~ another network; and

a ~~discarding unit~~ discarder configured to discard a message from a calling party of ~~the network element~~ a network where the apparatus is located to a called party of the ~~second~~ another network if a determination is made that there is no secure connection with said ~~second~~ another network.

31. (Currently Amended) ~~A network element~~ An apparatus, comprising:

determining means for determining, in a gateway ~~in a first network~~, if there is a secure connection with ~~a second~~ another network; and

discarding means for discarding a message from a calling party of ~~a first network~~ a network where the apparatus is located to a called party of ~~a second~~ the another network if a determination is made that there is no secure connection with said ~~second~~ another network.

32. (New) The apparatus as claimed in claim 21, wherein the first determiner is further configured to determine the address contained in a message for said called party.

33. (New) The apparatus as claimed in claim 32, wherein the message comprises a packet form.

34. (New) The apparatus as claimed in claim 21, wherein the second determiner is further configured to check if the address is contained in a database of trusted networks.

35. (New) The apparatus as claimed in claim 34, wherein the second determiner is further configured to check if the address is contained in said database in said network where the apparatus is located.

36. (New) The apparatus as claimed in claim 34, wherein the database is provided in a call session control function or a security gateway.

37. (New) The apparatus as claimed in claim 34, wherein said database comprises domain names associated with the trusted networks and internet protocol addresses of the trusted networks.

38. (New) The apparatus as claimed in claim 21, wherein the first determiner is further configured to determine if the address contains a domain name.

39. (New) The apparatus as claimed in claim 38, wherein if a determination is made that the address does not contain the domain name, the first determiner is further configured to send a request for the domain name.

40. (New) The apparatus as claimed in claim 39, wherein the first determiner is further configured to send said request to a domain name server.

41. (New) The apparatus as claimed in claim 38, wherein if a determination is made that the address does not contain the domain name, the first determiner is further configured to assume that the called party is in an untrusted network.

42. (New) The apparatus as claimed in claim 21, wherein if the called party is not in the trusted network, the controller is further configured to discard at least one message for the called party.

43. (New) The apparatus as claimed in claim 21, wherein the controller is further configured to modify said at least one message for the called party by removing identity information relating to said calling party.

44. (New) The apparatus as claimed in claim 43, wherein the controller is further configured to remove said identity information comprising a p-asserted-identity header.

45. (New) The apparatus as claimed in claim 21, wherein the second determiner is further configured to determine if a connection from a calling network to a called network is secured.

46. (New) The apparatus as claimed in claim 45, further comprising a gateway of the calling network.

47. (New) The apparatus as claimed in claim 45, wherein the gateway of the called network comprises a secure connection.

48. (New) The apparatus as claimed in claim 27, further comprising a gateway.

49. (New) The apparatus as claimed in claim 48, further comprising a security gateway.

50. (New) A computer program, embodied on a computer-readable medium, configured to control a processor to implement a method, the method comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message.

51. (New) A computer program, embodied on a computer-readable medium, configured to control a processor to implement a method, the method comprising:

determining, in a first network, if there is a secure connection with a second network; and

modifying a message from a calling party of the first network to a called party of the second network if a determination is made that there is no secure connection with said second network.

52. (New) A computer program, embodied on a computer-readable medium, configured to control a processor to implement a method, the method comprising:

determining, in a gateway in a first network, if there is a secure connection with a second network; and

discarding a message from a calling party in a first network to a called party in a second network, if a determination is made that there is no secure connection with said second network.